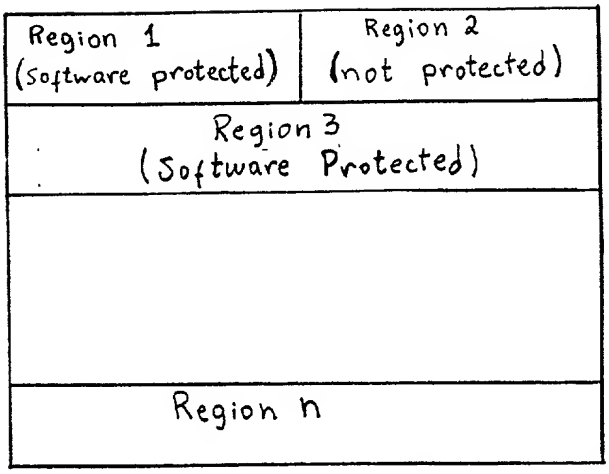

Figure 1

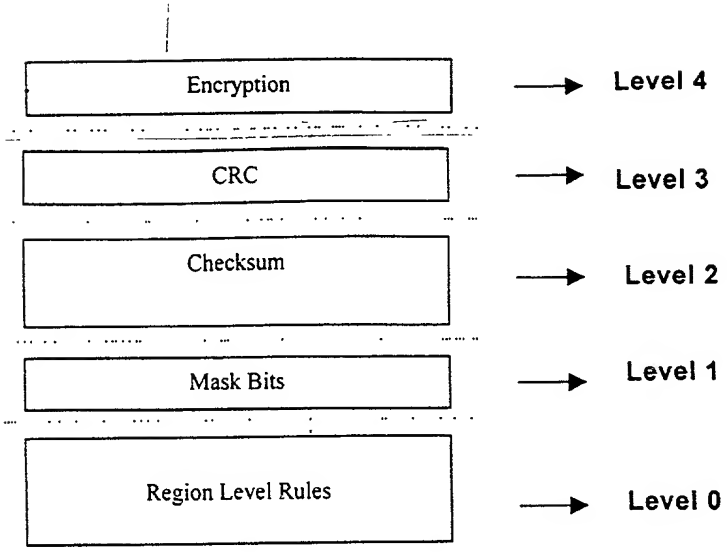

Figure 2

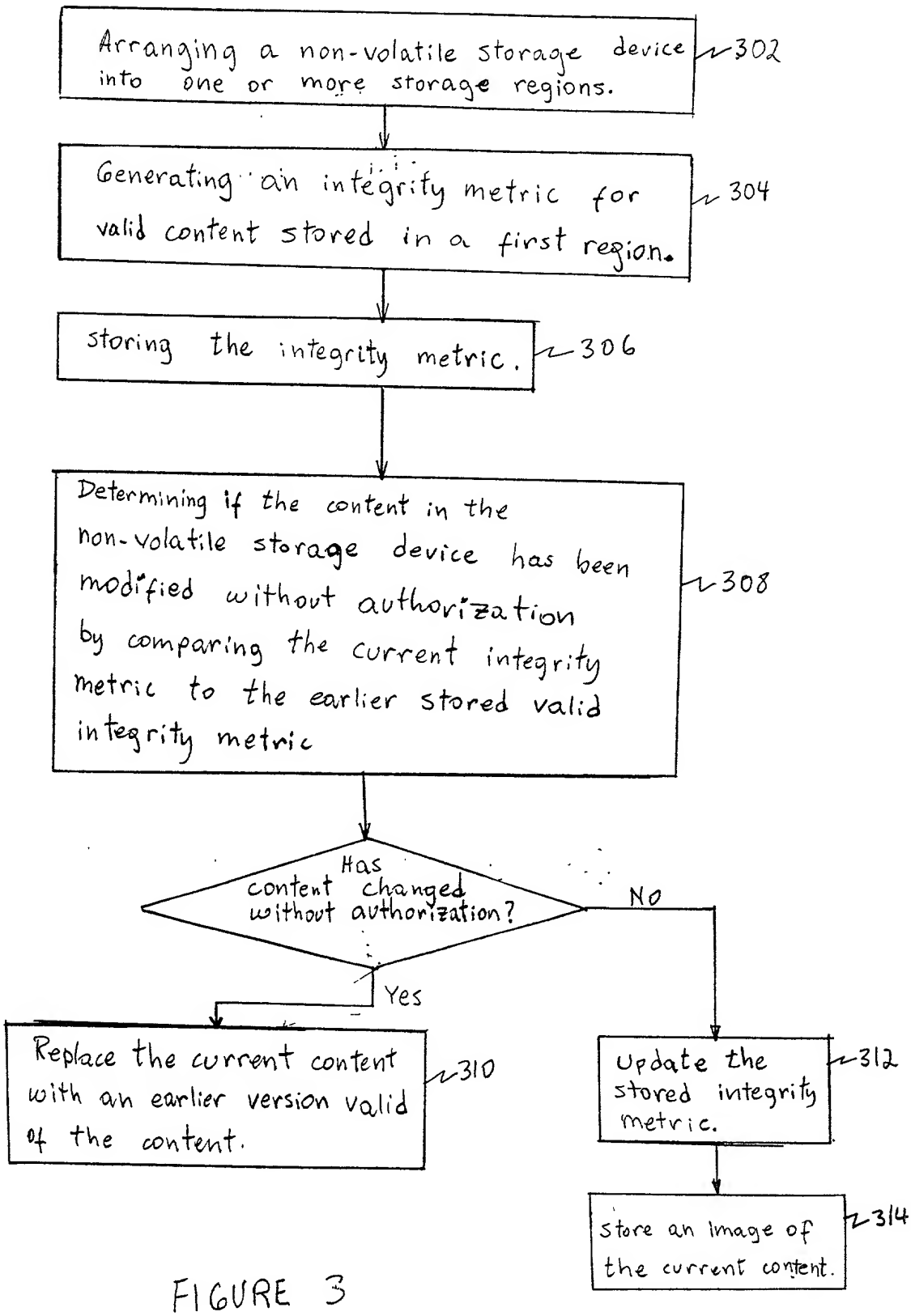
Arranging a non-volatile storage device into one or more storage regions.
302
Generating an integrity metric for valid content stored in a first region.
304
Storing the integrity metric.
306
Determining if the content in the non-volatile storage device has been modified without authorization by comparing the current integrity metric to the earlier stored valid integrity metric
308
Has content changed without authorization?
NO
Yes
Replace the current content with an earlier version valid of the content.
310
Update the stored integrity metric.
312
Store an image of the current content.
314

FIGURE 3

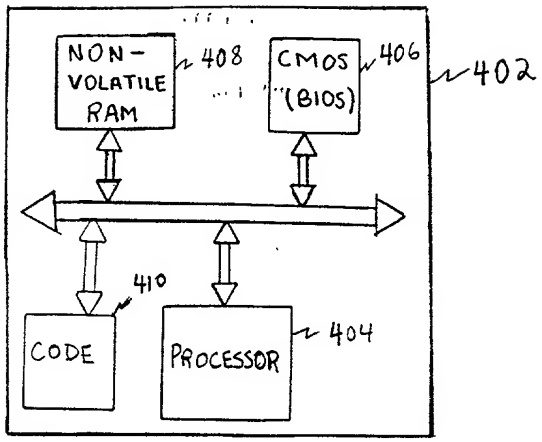

FIGURE 4

Page 56 of 70 - 10/5/2005 12:09:56 PM

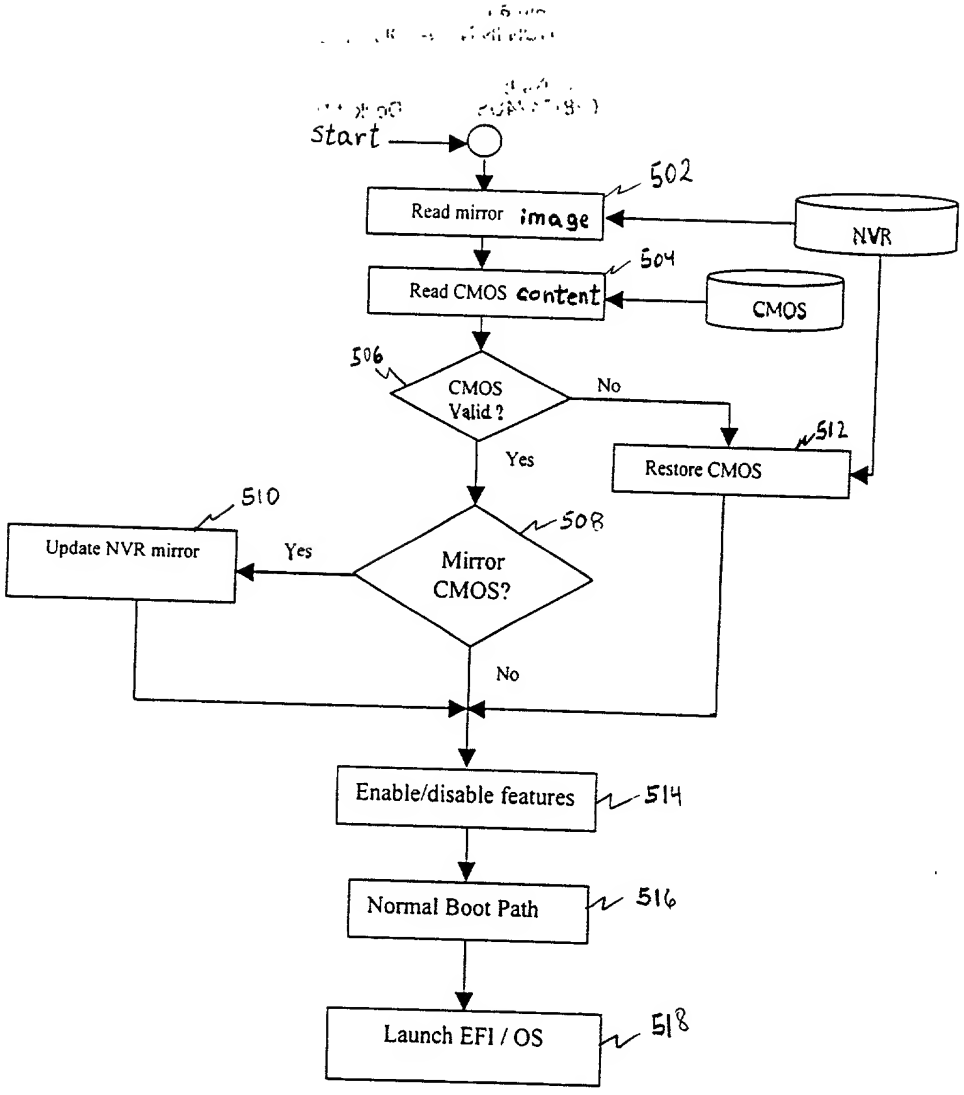
Start
Read mirror image
502
NVR
Read CMOS content
504
CMOS
506
CMOS Valid?
No
Yes
512
Restore CMOS
510
Update NVR mirror
Yes
508
Mirror CMOS?
No
Enable/disable features
514
Normal Boot Path
516
Launch EFI / OS
518

FIGURE 5